MASSACHUSETTS DEPARTMENT OF REVENUE

TY2008
Bulk E-Filer Registration and Transmission Guide

Massachusetts Department of Revenue
Information Services Organization
Updated: **9/12/2008**

Table of Contents

Overview

This document describes the Massachusetts Department of Revenue’s secure Internet-based method for filing corporate and individual bulk tax returns, bank match data, and other files containing taxpayer information. This method requires the use of SSH client software and registration as a Professional Tax Preparer (PTP) with bulk filer option on the WebFile for Business site. The WebFile for Business site is used as a central interface for registration and file tracking.

We have endeavored to make the registration and transmission process as simple as possible without compromising security. The following sections describe the registration and transmission processes.

Registration Process

You may or may not already be registered with WebFile for Business. Choose the topic below that best matches your current registration status with the WebFile for Business site.

My Company is Already Registered as a PTP with Bulk Filer Option

You need to update your service company information with an SSH-generated public key. Go to the section titled “*Update My SSH-Generated Public Key”***.**

My Company is Already Registered as a PTP But Without Bulk Filer Option

To upgrade your status with the Bulk Filer option:

1. Login to WebFile for Business: https://wfb.dor.state.ma.us/webfile/business

2. Choose the “Contact DOR” link

3. On the Contact DOR form, choose the “I am a PTP and want to register for Bulk File Transfer” category, submit the request.

4. You will receive an email when the request is approved.

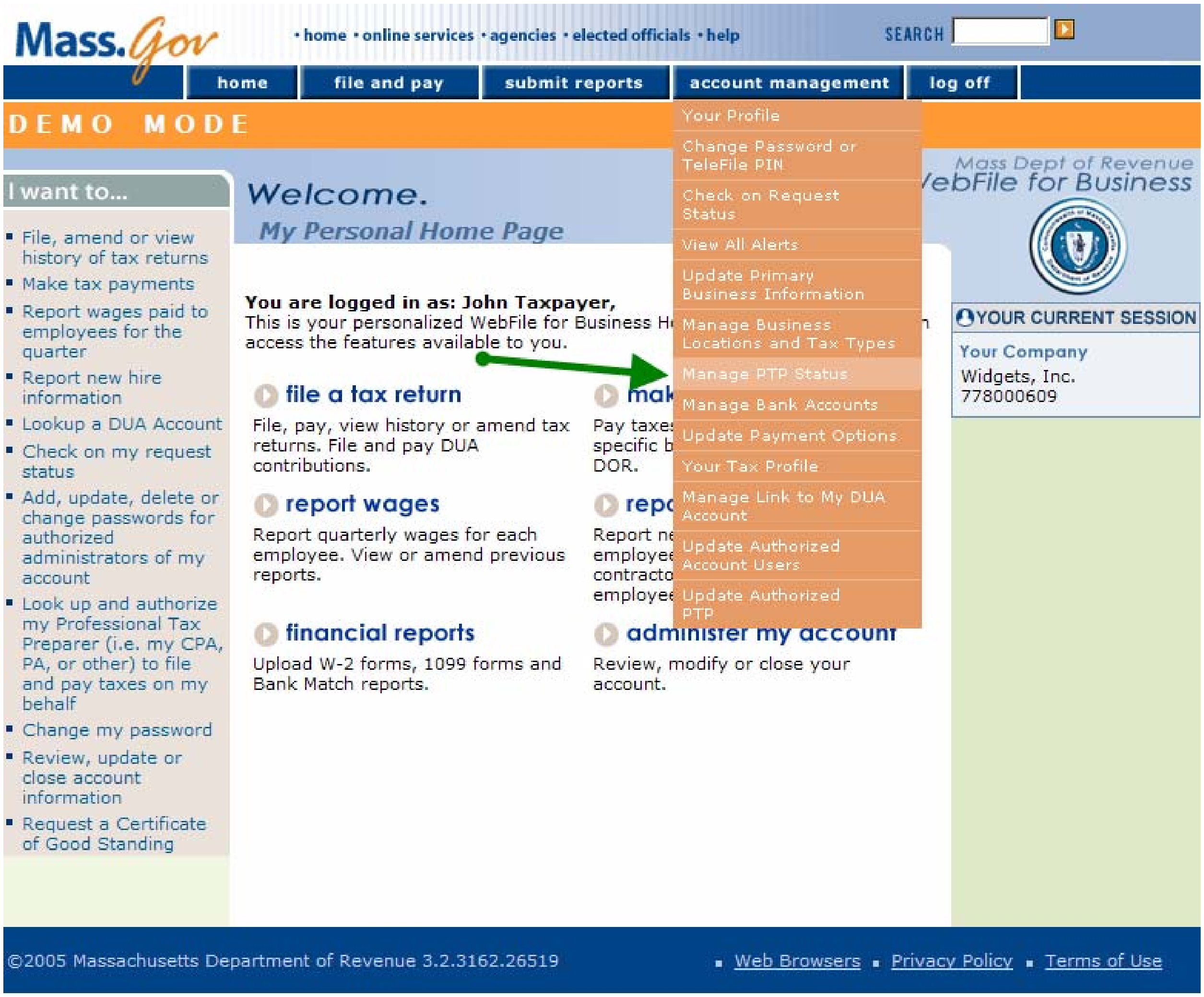
5. Once you have received the approval email, log back in and proceed to update your SSH-generated public key. Go to the section titled “*Update Your SSH-Generated Public Key”* for instructions.

My Company is Registered as a Taxpayer, But Not as a PTP

You can activate your company as Professional Tax Preparer, and then request bulk filer status. To do so:

1. Login to WebFile for Business: https://wfb.dor.state.ma.us/webfile/business

2. From the “Account Management” menu or section page, choose the “Manage PTP Status” option.


Mass.Gov
• home • online services • agencies • elected officials • help
SEARCH
home
file and pay
submit reports
account management
log off
DEMO MODE
Your Profile
Change Password or TeleFile PIN
Check on Request Status
View All Alerts
Update Primary Business Information
Manage Business Locations and Tax Types
Manage PTP Status
Manage Bank Accounts
Update Payment Options
Your Tax Profile
Manage Link to My DUA Account
Update Authorized Account Users
Update Authorized PTP
Mass Dept of Revenue
WebFile for Business
I want to...
File, amend or view history of tax returns
Make tax payments
Report wages paid to employees for the quarter
Report new hire information
Lookup a DUA Account
Check on my request status
Add, update, delete or change passwords for authorized administrators of my account
Look up and authorize my Professional Tax Preparer (i.e. my CPA, PA, or other) to file and pay taxes on my behalf
Change my password
Review, update or close account information
Request a Certificate of Good Standing
Welcome.
My Personal Home Page
file a tax return
mak
report wages
repo
financial reports
administer my account
YOUR CURRENT SESSION
Your Company
Web Browsers
Privacy Policy
Terms of Use

You are logged in as: John Taxpayer,
This is your personalized WebFile for Business H
access the features available to you.

File, pay, view history or amend tax returns. File and pay DUA contributions.

Pay taxes specific b DOR.

Report quarterly wages for each employee. View or amend previous reports.

Report ne employee contracto employee

Upload W-2 forms, 1099 forms and Bank Match reports.

Review, modify or close your account.

Widgets, Inc.
778000609

©2005 Massachusetts Department of Revenue 3.2.3162.26519

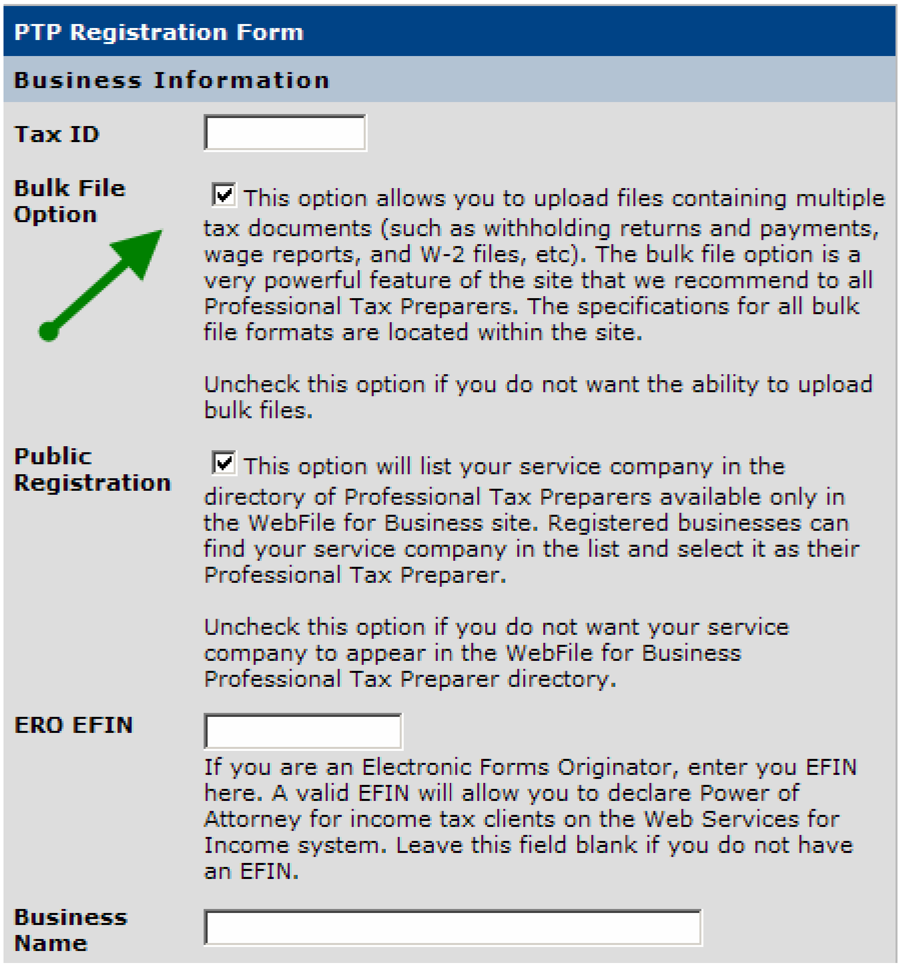
3. Fill out the form and click the Register button. This enables your registration status immediately.

4. You must now request Bulk Filer status. Follow the steps under the section "*My Company is Already Registered as a PTP But Without Bulk Filer Option*".

My Company is Not Registered With WebFile for Business

To register as a Professional Tax Preparer:

1. Point your browser at https://wfb.dor.state.ma.us/webfile/business Click the **Register** link under the "***I want to***" menu and follow the instructions for registering as a Professional Tax Preparer, and/or a Bulk File Transmitter. Make sure you select the Bulk Filer option on the registration page—otherwise you will have to make a separate request later.



PTP Registration Form

Business Information

Tax ID	
Bulk File Option	☑ This option allows you to upload files containing multiple tax documents (such as withholding returns and payments, wage reports, and W-2 files, etc). The bulk file option is a very powerful feature of the site that we recommend to all Professional Tax Preparers. The specifications for all bulk file formats are located within the site. Uncheck this option if you do not want the ability to upload bulk files.
Public Registration	☑ This option will list your service company in the directory of Professional Tax Preparers available only in the WebFile for Business site. Registered businesses can find your service company in the list and select it as their Professional Tax Preparer. Uncheck this option if you do not want your service company to appear in the WebFile for Business Professional Tax Preparer directory.
ERO EFIN	If you are an Electronic Forms Originator, enter you EFIN here. A valid EFIN will allow you to declare Power of Attorney for income tax clients on the Web Services for Income system. Leave this field blank if you do not have an EFIN.
Business Name	

2. When your registration request is approved, you will receive an email. Approval may take up to a full day, as the process is not automated.

3. Upon receipt of your registration activation email, follow the steps under the section "*Update My SSH-Generated Public Key*".

Update Your SSH-Generated Public Key

To update your SSH Public Key, you must be registered as a Professional Tax Preparer with Bulk Filer option, and you must have an SSH client which can generate the Public Key. If you do not have an SSH client and/or do not know how to generate the key, follow the steps under the section "*Obtaining and Configuring SSH and Public Key Generation*".

Once you have generated your key, take the following steps on the WebFile for Business site:

1. Login to WebFile for Business: https://wfb.dor.state.ma.us/webfile/business

2. From the "Account Management" menu or section page, choose the "Manage PTP Status" option.

3. Click the Update Certificate button.

4. Paste the Public Key generated by the SSH client into the text box labeled “New Public Key Certificate” and click Set Certificate.

If your key was not in the correct format or did not update successfully, you will see an error message. Otherwise your key has been successfully updated. This key must be the one you use when transmitting files to the DOR via SSH. Unlike the initial registration process, the process of submitting a key is fully automatic and instantaneous: once you submit a key, you can use that key immediately to connect with the MDOR.

Obtaining and Configuring SSH and Public Key Generation

File transfers to DOR are done using the SSH (Secure Shell) protocol, which provides strong encryption and authentication of file transfers. An SSH client is necessary in order to transfer your files to DOR. There are a variety of commercial and open source SSH clients to choose from. Commercial products include SSH Tectia Client and Ipswitch WS_FTP Professional 2007. OpenSSH and Putty are popular open source choices.

DOR will do its best to assist bulk filers with issues transferring files to DOR, but cannot assist users with issues installing and configuring their SSH software. **Support for installation and configuration should be directed to the vendor’s customer support**.

If you are having problems with a particular SSH client, please see the section entitled “*Support Information and Notes for Various SSH Client Software”* below.

There are five steps that need to be completed before using SSH to send files to DOR:

1. Installing the SSH software
2. Generating a public/private keypair
3. Configuring an SSH client to use Public-key authentication
4. Copying your public key to the clipboard
5. Pasting your public key into your Webfile for Business site

Installing the SSH Software

Here, we’ll only deal with the SSH Tectia Client version 6.0 running on Windows. You’ll have to consult your vendor or other sources for installation of other versions of SSH and other operating systems.

Generating a Public/Private Keypair

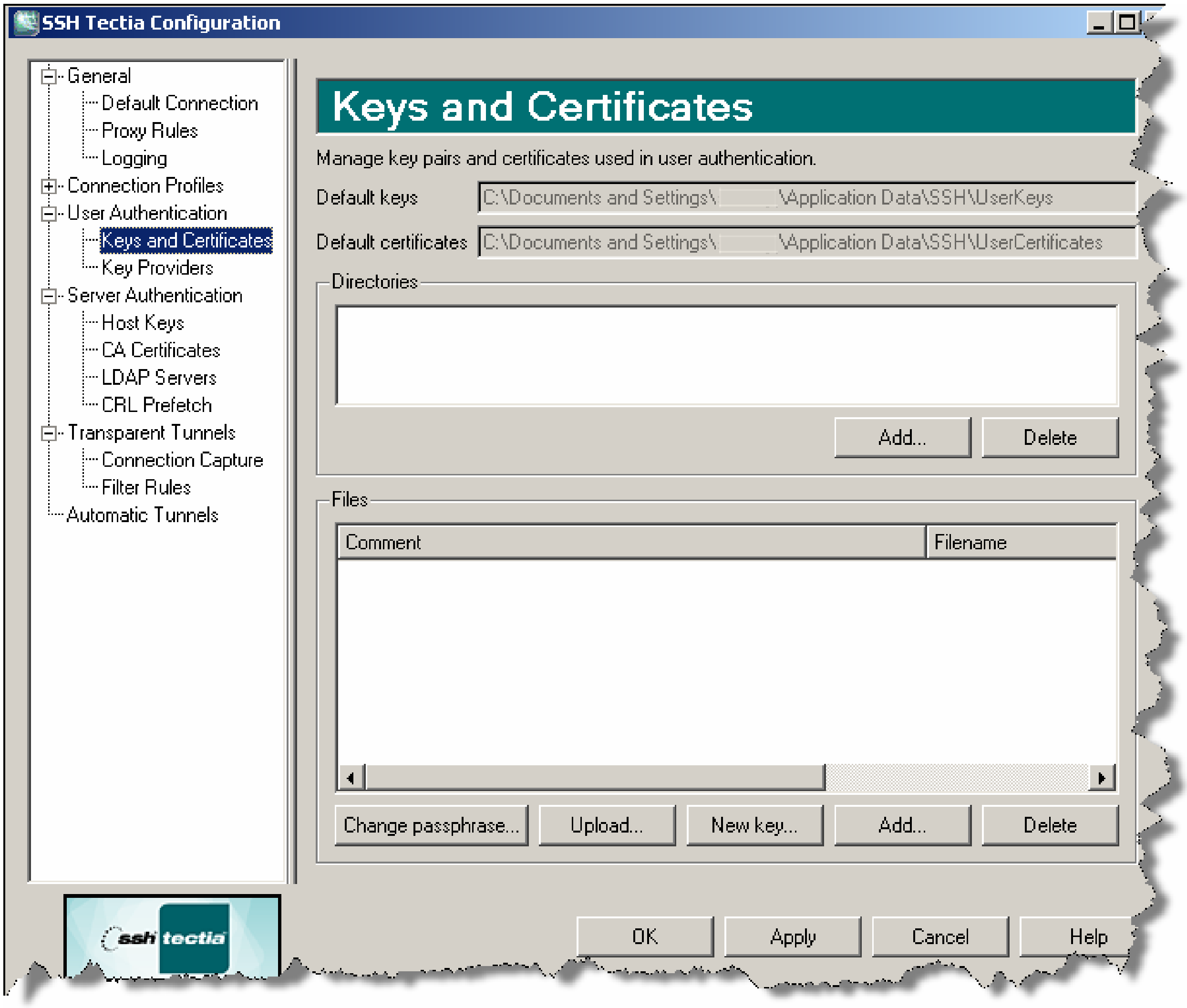
The next step is to generate your public/private key pair. The easiest way to do this with SSH Tectia Client is to use the key-generation facilities of the SSH Tectia graphical user interface (“GUI”):

- Start up the SSH Tectia Client GUI by navigating to Start→Programs→SSH Tectia Client→SSH Tectia Configuration

- Under the ‘Profiles’ menu, select ‘Edit Profiles’

- Select ‘User Authentication/Keys and Certificates’

- Click on the ‘New Key…’ button (see *Figure* 1.)



Keys and Certificates

Manage key pairs and certificates used in user authentication.

Default keys: C:\Documents and Settings\ \Application Data\SSH\UserKeys

Default certificates: C:\Documents and Settings\ \Application Data\SSH\UserCertificates

Figure 1

- Follow the instructions on the dialog box, accepting default settings for Key type (default = DSA) and Key length (default = 2048). The actual key generation step may take a few minutes.

- When the process completes, you are asked to click ‘Next’ to continue. Do so, and you’ll be asked for some information about your new key. The Filename and Comment values are arbitrary. ***The Passphrase fields may be left blank. If you choose to enter a passphrase, it will be used to encrypt your *private* key file on your local computer, and you will be required to type in the passphrase every time*** **you** ***connect to the DOR.***

  The key-creation wizard will give a warning if you choose not to protect your key with a passphrase, but it will allow it.

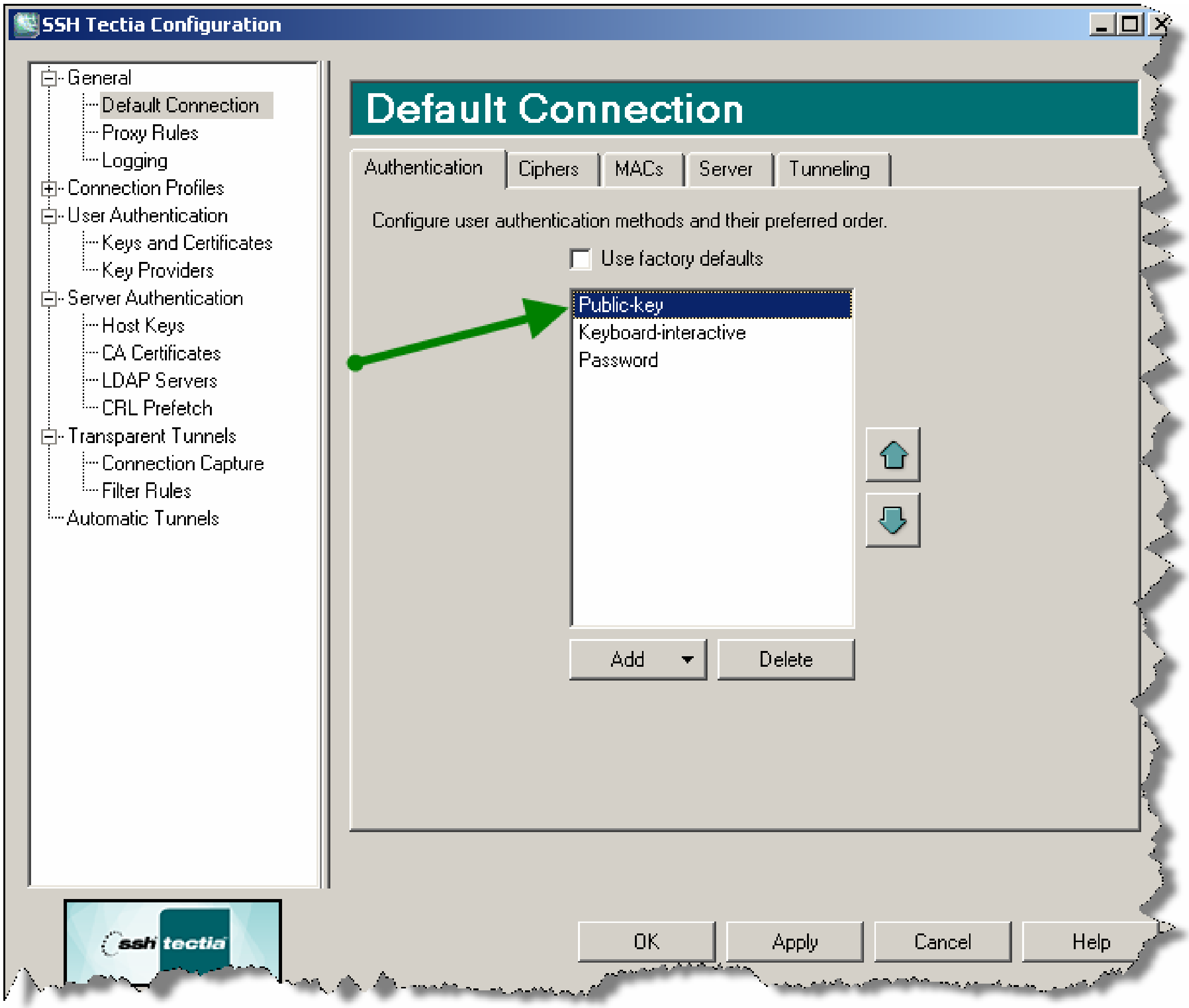
  Passphrases are discussed in detail in the “*Troubleshooting/Frequently Asked Questions”* and *“Additional Information on Passphrases and Passwords”* sections of this document.

- Fill in the dialog as required, and click on ‘Next’.

- Click on the ‘OK’ button. The ‘Upload...’ function is of no use here.

Configuring SSH Tectia Client to Use Public-key Authentication

Your SSH Tectia Client may already be set up to use Public-key authentication, but you should verify this. Go to the Profiles button and click Edit Profiles. Under General, click Default Connection, then select the Authentication tab. This will show you a list of user authentication methods. If "Public-key" is not listed, add it to the list using the "Add" drop-down. Then, select the line “Public-key” and use the up-arrow button to move it to the top of the list of methods if it is not already there (*see Figure2.)* Click the OK button.



Configure user authentication methods and their preferred order.

□ Use factory defaults

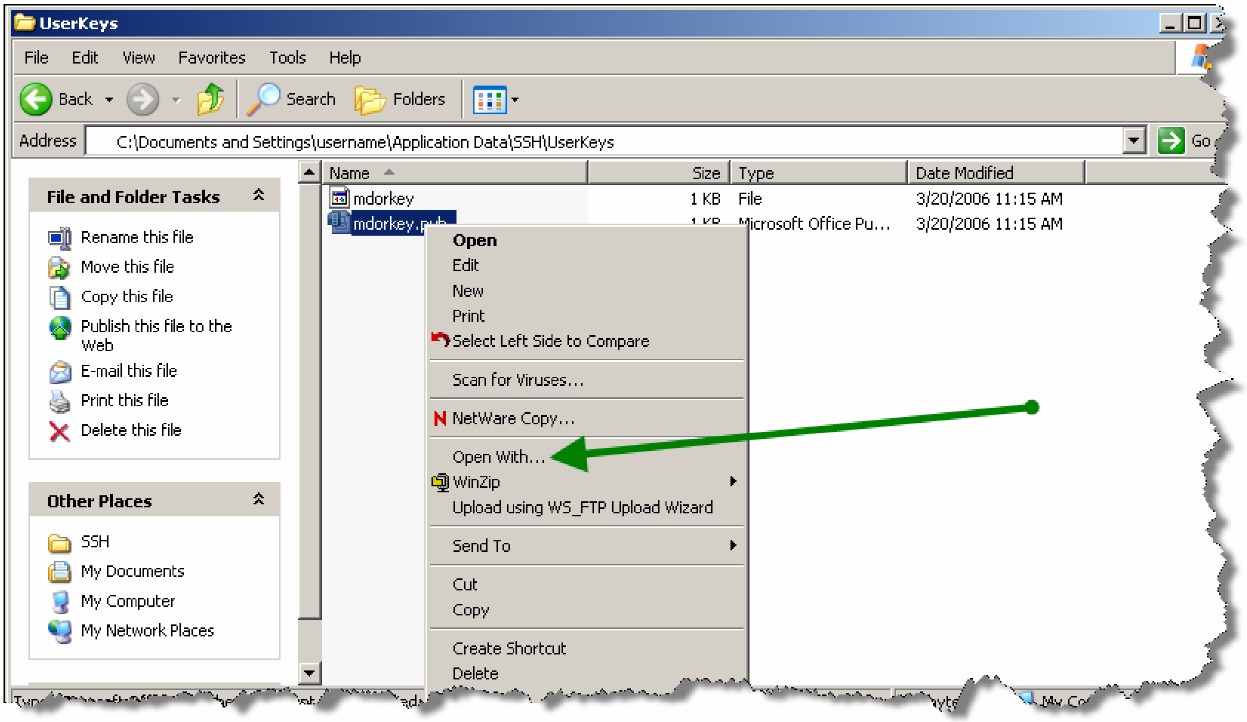
Public-key
Keyboard-interactive
Password

Figure 2

Copying Your Public Key to the Clipboard

To copy your public key to the clipboard in preparation for uploading it to WebFile for Business:

- Use Windows Explorer to browse to the directory containing your key files. For most versions of Windows, this will be C:\Documents and Settings\<your login name>\Application Data\SSH\UserKeys. For Windows Vista and Windows Server 2008, the directory will be C:\Users\<your login name>\Application Data\SSH\UserKeys. The directory will contain a pair of files containing the public-and-private key pair you generated; if you named your key pair "mdorkey", for instance, the file "mdorkey" contains the private key and "mdorkey.pub" contains the public key. Right-click the ".pub" file and open it with Wordpad *(see Figure 3.)*

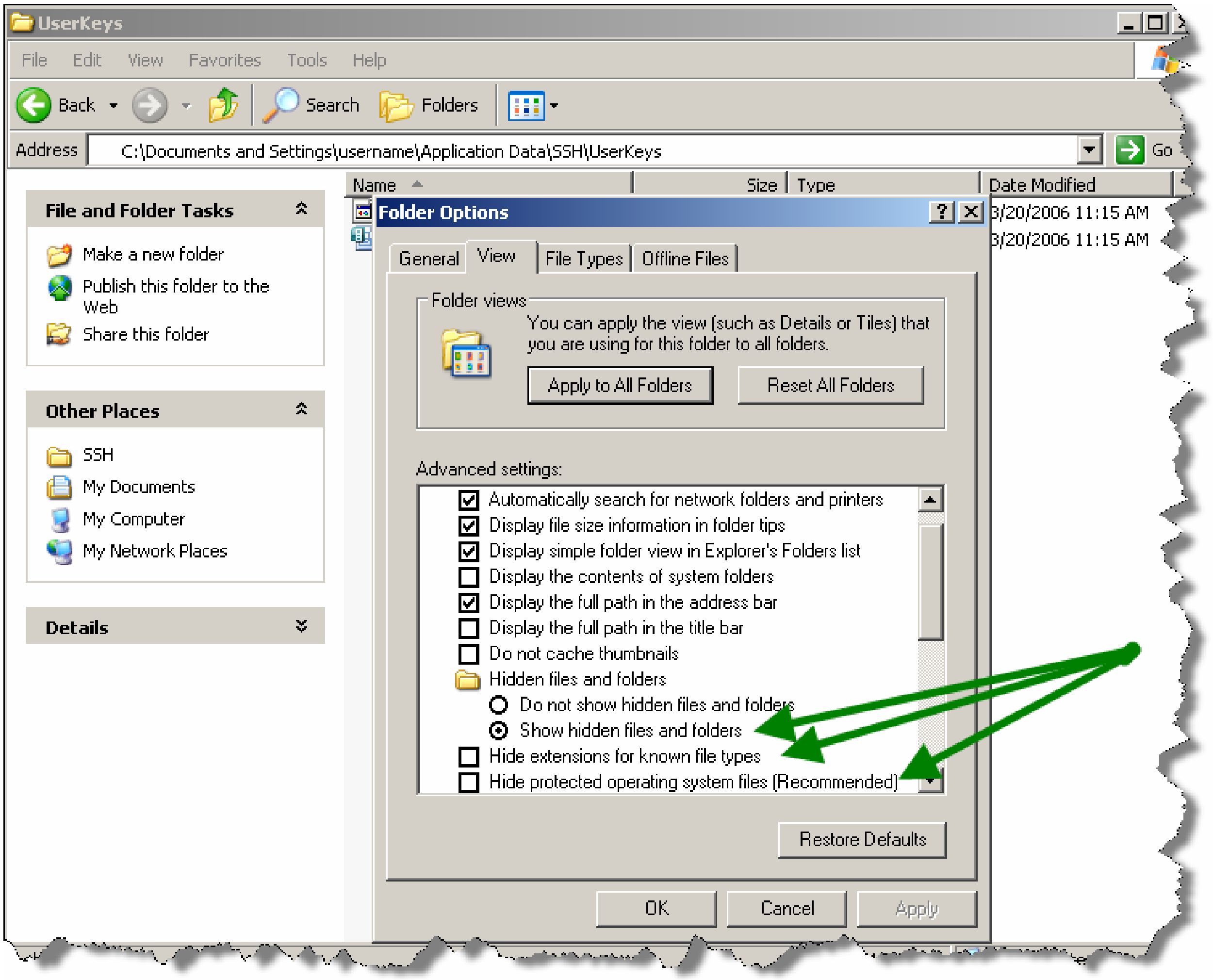


Address C:\Documents and Settings\username\Application Data\SSH\UserKeys

Name	Size	Type	Date Modified
mdorkey	1 KB	File	3/20/2006 11:15 AM
mdorkey.pub	1 KB	Microsoft Office Pu...	3/20/2006 11:15 AM

Figure 3

- (**NOTE**: If you can't find the "Application Data" directory it is because your Windows Explorer is configured to hide sensitive files from you. To set up Explorer to display such files, look on the Tools menu, Folder options, the View tab, and check "show hidden files and folders". If that doesn't help, try unchecking "Hide protected operating system files". (*See Figure 4.*)



Address: C:\Documents and Settings\username\Application Data\SSH\UserKeys

3/20/2006 11:15 AM
3/20/2006 11:15 AM

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

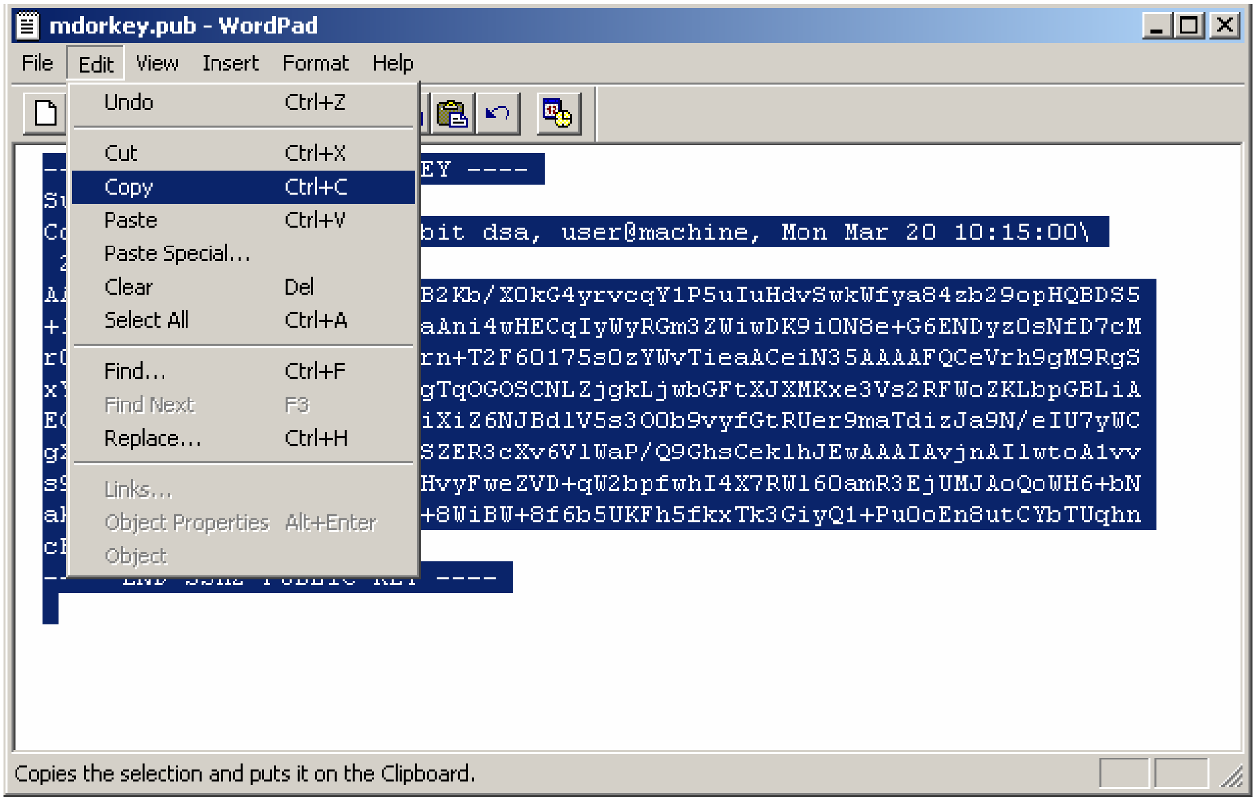
- ☑ Automatically search for network folders and printers
- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- ☐ Display the contents of system folders
- ☑ Display the full path in the address bar
- ☐ Display the full path in the title bar
- ☐ Do not cache thumbnails
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- ☐ Hide extensions for known file types
- ☐ Hide protected operating system files (Recommended)

Figure 5

- In Wordpad, select the entire content of the file with the mouse. Make sure you include the lines containing “BEGIN SSH2 PUBLIC KEY” and “END SSH2 PUBLIC KEY”. Alternatively, hold down the control key and press the ‘A’ key, which should select the whole file. (*See Figure 5.*)

- Under the ‘Edit’ menu, select ‘Copy’

Now paste the key into WebFile for Business as detailed in the section above entitled “*Update Your SSH-Generated Public Key*”.



```
--                EY ----
Su
Co                bit dsa, user@machine, Mon Mar 20 10:15:00\
 2
AA                B2Kb/XOkG4yrvcqY1P5uIuHdvSwkWfya84zb29opHQBDS5
+1                aAni4wHECqIyWyRGm3ZWiwDK9iON8e+G6ENDyzOsNfD7cM
r0                rn+T2F6O175sOzYWvTieaACeiN35AAAAFQCeVrh9gM9RgS
xY                gTqOGOSCNLZjgkLjwbGFtXJXMKxe3Vs2RFWoZKLbpGBLiA
E0                iXiZ6NJBdlV5s3OOb9vyfGtRUer9maTdizJa9N/eIU7yWC
gX                SZER3cXv6V1WaP/Q9GhsCeklhJEwAAAIAvjnAIlwtoA1vv
s9                HvyFweZVD+qW2bpfwhI4X7RW16OamR3EjUMJAoQoWH6+bN
ak                +8WiBW+8f6b5UKFh5fkxTk3GiyQ1+PuOoEn8utCYbTUqhn
cF
--                ----
```

Copies the selection and puts it on the Clipboard.

Figure 5

Transmission of Files

Login ID

Once your public key has been uploaded to DOR, you should be able to begin transferring files. Your login ID is your FID prefixed by the letters “FID”. For example, if your FID is 121212121, then your SSH login ID (also known as a “username”) would be: FID121212121. **Do not use your WFB login id as your SSH username.**

File Naming Convention/File Compression

Files should be named according to their type. Extensible Markup Language files should use the extension “.xml”. Text files (ASCII or EBCDIC) should use the extension “.txt”. Each file name should be unique, and include the FID number used to log into the SSH server, as well as a date (4 digit year) and time (24 hour clock). Note: For batch filers, the FID numbers within wage reporting and wage withholding files are not assumed to be the same as the FID numbers used to log into SSH or as part of the filename. Beyond the FID, timestamp and extension, file names must conform to the rules required for the specific filing. Files may be sent compressed or uncompressed, although compression is preferred to conserve on network bandwidth. Compress files with any of the following: gzip, bzip, Winzip, PKZIP, UNIX compress.

Note: The term “FID” is synonymous with “EIN”.

Testing Connectivity to DOR

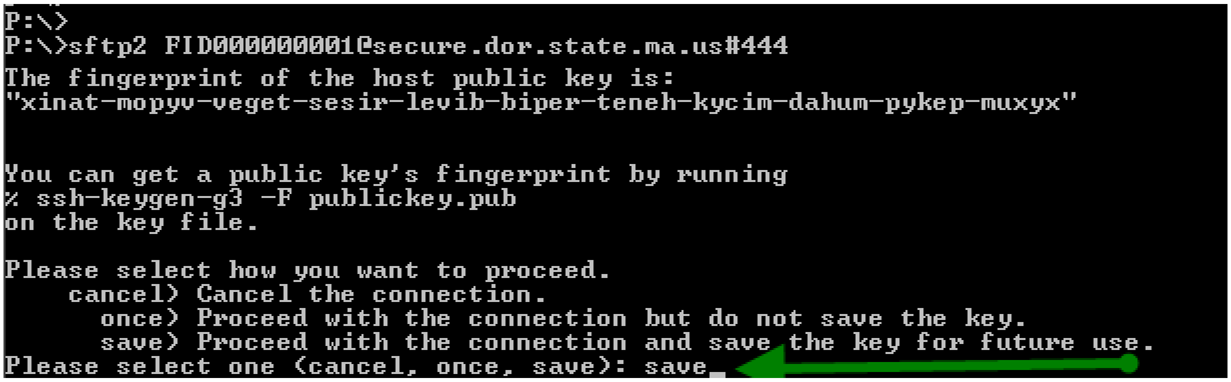
If you're using the SSH Tectia Client, transfers to DOR can be done using either scp2 or sftp2. sftp2 can be used to test connectivity to DOR by following these steps:

If you’re running on Windows obtain a command prompt by navigating to Start→Programs→Accessories→Command Prompt.

Enter the following command at a command prompt:

```
sftp2 username@secure.dor.state.ma.us#444
```

where “*username*” is replaced by your SSH login ID (*e.g.*, FID121212121). The first time you connect to DOR's SSH server, you will be prompted by your SSH client to save the new host key. You should answer "save" here (see Figure 6).



```
P:\>
P:\>sftp2 FID000000001@secure.dor.state.ma.us#444
The fingerprint of the host public key is:
"xinat-mopyv-veget-sesir-levib-biper-teneh-kycim-dahum-pykep-muxyx"


You can get a public key's fingerprint by running
% ssh-keygen-g3 -F publickey.pub
on the key file.

Please select how you want to proceed.
    cancel) Cancel the connection.
      once) Proceed with the connection but do not save the key.
      save) Proceed with the connection and save the key for future use.
Please select one (cancel, once, save): save
```

Figure 6

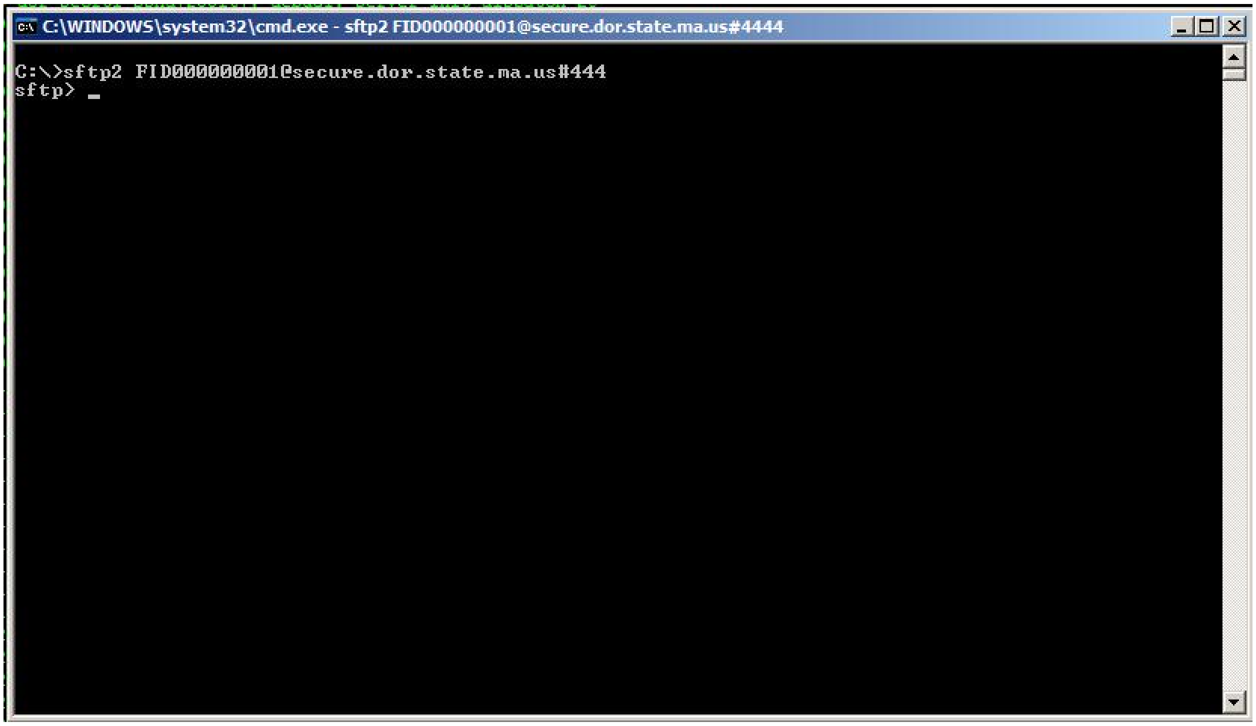
Your SSH client will warn you if it detects a different host key in subsequent transfer attempts (which may mean that an unauthorized attempt is being made to eavesdrop on your communication with DOR).

DOR's public-key fingerprint is:
xinat-mopyv-veget-sesir-levib-biper-teneh-kycim-dahum-pykep-muxyx

Consult the documentation for your SSH client to determine how to use this information to confirm that the site that you've connected to is indeed DOR and has the correct public key.

After accepting the new host key, you should be presented with an “sftp>” prompt that looks like *Figure 7* If you receive an error, or you are not presented with the “sftp>” prompt, please refer to the “*Troubleshooting/Frequently Asked Questions”* section below.

Note that, for security reasons, the only directories you will have access to are the “upload” and “download” directories. The only command that is allowed within the “upload” directory is “put”, so you will not be able to do a directory listing in the “upload” directory. The only commands allowed in the “download” directory are “ls”, “get” and “mget”, so you will not be able to “put” or “rename” files in the “download” directory.


C:\WINDOWS\system32\cmd.exe - sftp2 FID000000001@secure.dor.state.ma.us#4444

```
C:\>sftp2 FID000000001@secure.dor.state.ma.us#444
sftp> _
```

Figure 7

Transfers to DOR (Uploads)

Transfers to and from DOR are performed from a *command line*. **THE GUI THAT COMES WITH SSH TECTIA CLIENT CANNOT BE USED TO TRANSFER FILES TO DOR.**

If you're using the SSH Tectia Client, transfers to DOR can be done using either scp2 or sftp2. The following is the syntax for these two commands.

Note: The following commands should be typed on *one single* command line, although in the examples below the command may wrap onto a second line.

Scp2:

Syntax:	`scp2 [filename] [username]@[server]#[port]:upload/[filename]`
Example:	`scp2 MA9411212121212120030101145959.xml FID121212121@secure.dor.state.ma.us#444:upload/MA9411212121212120030101145959.xml`

Sftp2 (batch mode):

Syntax:	`sftp2 -B [batchfile] [username]@[server]#[port]`
Example:	`sftp2 -B work.bat FID121212121@secure.dor.state.ma.us#444`

Sftp2 (interactive mode):

Syntax:	`sftp2 [username]@[server]#[port]`
Example:	`sftp2 FID121212121@secure.dor.state.ma.us#444`

`[filename]`	Name of file to transfer.
`[username]`	FID. Example: FID121212121
`[server]`	DOR server = secure.dor.state.ma.us.
`[port]`	Port to connect to. DOR uses port 444.
`[batchfile]`	A file with the following FTP commands:

	`cd upload`
	`put [filename]`
	`quit`

An example batch file would look like this:

```
cd upload
put MA94112121212120030101145959.xml
quit
```

Note: You only need to create a batch file if you intend to run sftp2 from a batch script.

Transfers from DOR (Downloads)

Downloads are similar to uploads to DOR, but the order of the remote and local filenames is reversed for scp2 commands, and files available for download are in a directory with a name that matches your login ID (*e.g.,* FID121212121) under the general “download” directory.

In addition to the direct path examples provided below, you will be able to list files by doing "ls", and to download multiple files with the "mget" command. For example, "ls download/FID121212121", and "mget download/FID121212121/*".

If there are no files available, the "download/username" directory may not exist. It only gets created when files are ready for download. You will need to handle this if you are using automated scripts.

Examples of direct path, single file retrieval:

Scp2

Syntax:	`scp2 [username]@[server]#[port]:download/FID121212121/[filename] [filename]`
Example:	`scp2 FID121212121@secure.dor.state.ma.us#444:download/FID121212121/MA94112121212120030101145959.xml MA94112121212120030101145959.xml.ack`

Sftp2

Syntax:	`Sftp2 -B [batchfile] [username]@[server]#[port]`
Example:	`Sftp2 -B work.bat FID121212121@secure.dor.state.ma.us#444`

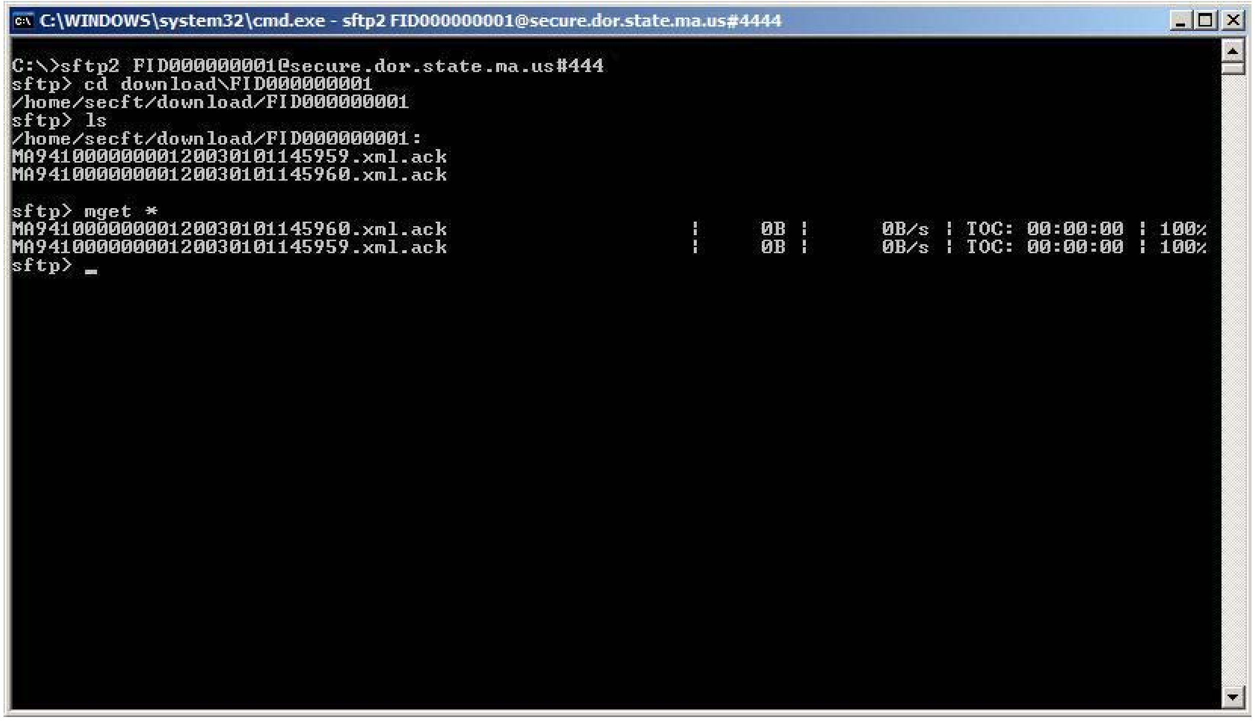
`[filename]`	Name of file to transfer.
`[username]`	FID. Example: FID121212121
`[server]`	DOR server = secure.dor.state.ma.us.
`[port]`	Port to connect to. DOR uses port 444.

`[batchfile]`	A file with the following FTP commands:
	`cd download\`*`username`*
	`get [filename]`
	`Quit`

An example batch file would look like this:

```
cd download\FID121212121
get MA9411212121212120030101145959.xml.ack
quit
```

Figure 86. shows an interactive sftp2 session doing a directory listing and an “mget” of multiple files:


C:\WINDOWS\system32\cmd.exe - sftp2 FID000000001@secure.dor.state.ma.us#4444

```
C:\>sftp2 FID000000001@secure.dor.state.ma.us#444
sftp> cd download\FID000000001
/home/secft/download/FID000000001
sftp> ls
/home/secft/download/FID000000001:
MA94100000000120030101145959.xml.ack
MA94100000000120030101145960.xml.ack

sftp> mget *
MA94100000000120030101145960.xml.ack                    |      0B |       0B/s | TOC: 00:00:00 | 100%
MA94100000000120030101145959.xml.ack                    |      0B |       0B/s | TOC: 00:00:00 | 100%
sftp> _
```

Figure 8

Troubleshooting/Frequently Asked Questions

Most of the problems that filers encounter with SSH-based file transfer stem from a few common misunderstandings. The items address the frequent problems that users encounter.

Throughout this section, the words "local" and "client" refer to computers and software operated by the filer, while "remote" and "server" refer to the computers and software at the Department of Revenue.

Q1: ***Why do I get an error saying "Could not open connection to 'username@secure.dor.state.ma.us#444': Authentication failed" when I try to use sftp2 or scp2 to connect to MDOR?***

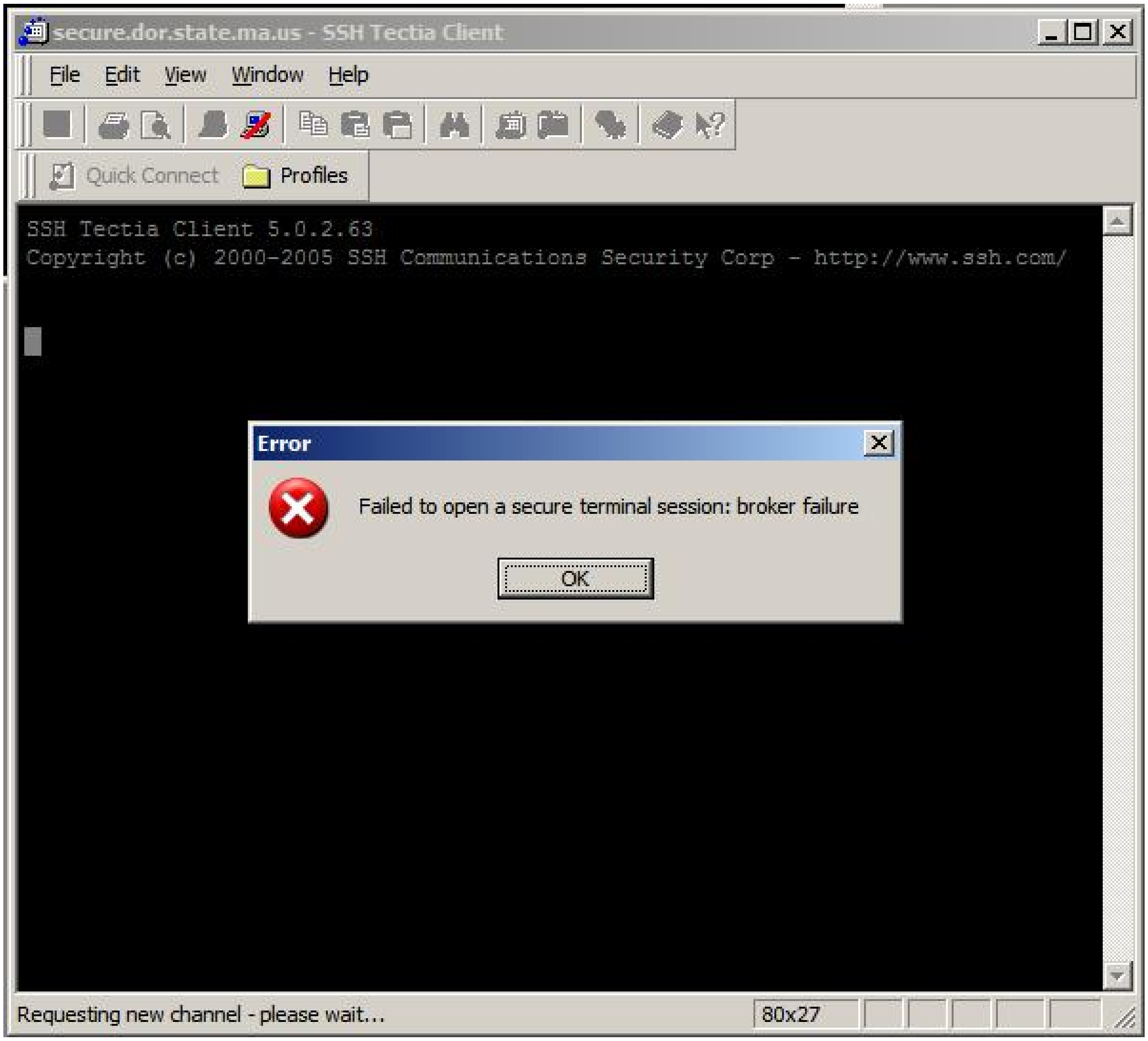
This question has several possible answers:

A1: Make sure you are specifying destination port number 444 in your scp2 or sftp2 command. *This is not the standard default port number for SSH-based connection, so your connection attempt will fail if you neglect to specify it.*

A2: There may be a firewall on your side blocking this connection. If you or your company has a firewall in place, contact the firewall administrator with the following information: The server "secure.dor.state.ma.us" has two IP addresses, 4.36.198.14 and 65.118.148.14. Your firewall should permit outbound TCP connections on port 444 to both of these addresses, because DNS may return either address at any given time.

A3: Make sure you are using the correct username to log in. Your SSH login username is "FIDnnn..." where "nnn..." is your 9-digit Filer ID. *Your SSH username is not the username you use to log in to the WFB Website.* The "FIDnnn..." username is created for you behind the scenes when you register your SSH public key.

Q4: ***When I try to connect I get an error saying "Failed to open a secure terminal session: broker failure"*** *(see Figure 97.)*



```
SSH Tectia Client 5.0.2.63
Copyright (c) 2000-2005 SSH Communications Security Corp - http://www.ssh.com/
```

Failed to open a secure terminal session: broker failure

Requesting new channel - please wait...

Figure 9

A4: You are attempting to use the SSH Tectia GUI interface instead of the command line tools. The GUI is not supported for file transfers on DOR's site and, in fact, the command-line tools scp2 and sftp2 sometimes get confused if the GUI client is even running at the same time. Although the GUI can be useful for creating the initial public/private key pair, *all connections and transfers should be performed using the command line tools (scp2 or sftp2)*.

Q5: ***When trying to send a file, I receive an error saying "Permission denied".***

A5: Make sure you are entering the destination directory correctly. All uploads go to the "uploads/" directory, and all downloads are performed from the "downloads/FIDnnn..." directory. Do *not* include a slash before the directory specification. "Permission denied" errors are frequently caused by problems with directory specifications. These directories and all of the scp2/sftp2 commands and arguments are case-sensitive. If the example says "FID", "fid" will not work. if the example says "upload", neither "UPLOAD" nor "Upload" will work.

Note that, for security reasons, the only directories you will have access to are the "upload" and "download" directories. The only command that is allowed within the "upload" directory is "put", so you will not be able to do a directory listing in the "upload" directory. The only commands allowed in the "download" directory are "ls", "get" and "mget", so you will not be able to "put" or "rename" files in the "download" directory.

Q6: Why is SSH Tectia Client asking me for my password/passphrase?

A6: Be careful to distinguish the words "password" and "passphrase"; they are not the same thing. A passphrase is a secret text string that is used to protect your private key on your local client workstation; a password is used to authenticate a user at the remote server, although DOR's SSH server does not allow users to authenticate with passwords.

Password Prompts

If you are prompted for a *password*, the cause is most likely one of two things:

1) Your public key was not correctly uploaded to Webfile for Business website. Please copy and paste it into Webfile for Business again, and repeat your attempt to connect.

or

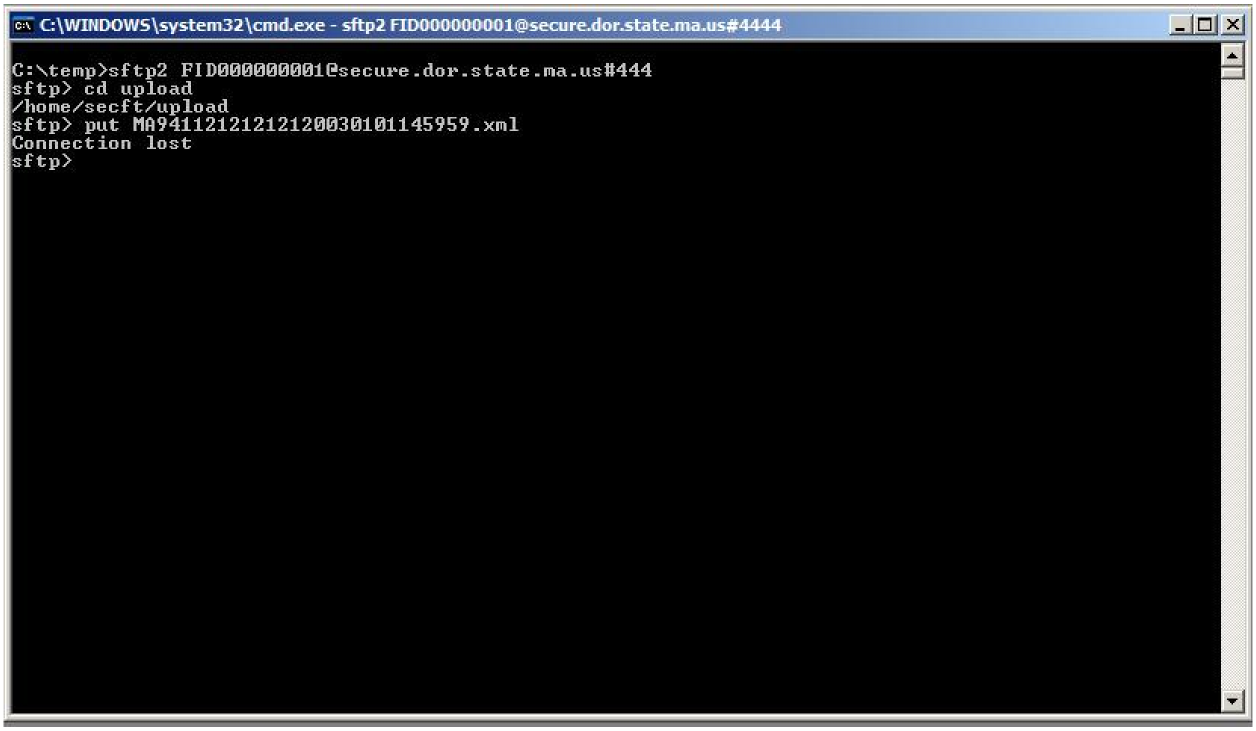
2) Your SSH client is not configured to use Public-key authentication. We have found that the order in which authentication methods are specified in the client can be important. If you are encountering authentication problems, go to Profiles/Edit Profiles/General/Defaults/Authentication and make sure that "Public Key" is listed first in the "Authentication methods" window (see *Figure 2* above).

Passphrase Prompts

If you are prompted to enter a *passphrase* when you attempt to connect to the MDOR server, the prompt is coming from your local client software. It means that when your keys were first created, the private key was encrypted with a passphrase which you will need to enter each time you connect to DOR.

See the section entitled "*Additional information on passphrases and passwords"* below for details.

Q7: When trying to send a file, I receive an error saying "Connection lost". (See Figure 10)


C:\WINDOWS\system32\cmd.exe - sftp2 FID000000001@secure.dor.state.ma.us#4444

```
C:\temp>sftp2 FID000000001@secure.dor.state.ma.us#444
sftp> cd upload
/home/secft/upload
sftp> put MA94112121212120030101145959.xml
Connection lost
sftp>
```

Figure 10

A7: This is a known issue with SSH Tectia Client when the “SSH Tectia Broker” is running. The “SSH Tectia Broker” is a software component that ships with SSH Tectia Client. It is configured to start up automatically when you log into your computer, and then continues to run in the background.

Check to see whether the Tectia Broker is running, and if it is, turn it off as follows: look in your System tray (the right side of the grey taskbar at the bottom of the monitor's window, near the clock display) for a blue-grey icon with a grid of white lines. Right-click on the icon and select "Exit" from the menu; the icon should disappear. (See *Figure 11*

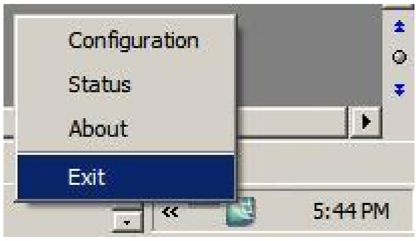


Figure 11

Q8: How can I get more information from the SSH Tectia Client about why it is failing?

A8: If file transfers are still not working, you can tell the scp2 or sftp2 program to display additional information by including a "debug" or "verbose" switch in the command, but be careful with the syntax. The scp2 program recognizes the "-v" switch, but the sftp2 program does not. Both programs, scp2 and sftp2, recognize the "-D 2" switch.

The debug switch must appear immediately after the program name (scp2 or sftp2) in the command line, before the "username@server" specification or before the "-B filename" specification. The switches are case-sensitive, lower case for "-v", upper case for "-D 2". You can use any number between 1 and 99 with the "-D" switch; higher numbers produce more detailed messages, but anything greater than 2 is likely overkill. Examples:

```
C:> scp2 -v MA9411212121212120030101145959.xml
FID121212121@secure.dor.state.ma.us#444:upload/

C:> sftp2 -D 2 -B upload.bat FID121212121@secure.dor.state.ma.us#444
```

Q9: ***It still doesn't work. Do you have any other advice?***

A9: Make sure it's really an error; some messages that say "error" can be ignored, and some "unexpected" behaviors are actually correct. For example, the "upload" directory is write-only, and you will not see your uploaded file if you 'ls' the directory. This advice applies particularly to the output from the "-D" and "-v" switches.

If you still can't find the problem, try to get a screen capture or text capture before contacting the DOR. If possible, show the command you are using and the output using the "-D 2" or "-v" switch. From a Windows Command Prompt window, you can right-click on the top control bar to get a menu with an "edit/select all" option, and copy the selected text into a text file in Notepad. Or you can select the relevant section of text from the Command Prompt window with the mouse.

Additional Information on Passphrases and Passwords

Passphrases: When you create your public/private key pair, you will be given the opportunity to assign a passphrase to protect the private key on your local client workstation. If you choose *not* to assign a passphrase, your private key will be stored in a file in plaintext on your local workstation, and anyone with physical or network access to the workstation could copy the private key file and use it in combination with your public key to impersonate you.

If you *do* assign a passphrase, your private key will be stored in a file in encrypted format. In this case, when the client software needs to read your private key, it will prompt you to enter the key's passphrase, and it will use the passphrase to decrypt the private key so that the file transfer can take place. Anyone who obtains your encrypted private-key file will find it useless without its accompanying passphrase.

The advantage to using a passphrase is that a passphrase makes your private key more secure. There are several disadvantages, though:

- As with any secret word, you have to remember it. The passphrase itself is not stored in any file, database, or registry, and if you forget it, there is no way to recover it - you will have to generate a new key pair and submit the new public key to DOR. If you write it down and put it in a drawer it becomes as vulnerable as any other written-down password.

- The rule "do not write down your passphrase" causes problems for scripting. Most filers want to automate the process of exchanging files with MDOR by writing scripts to control the scp2/sftp2 client, but there is no good way to incorporate the passphrase into a script file.

There isn't much that can be done about the first of these difficulties, but there are partial solutions for the second. Both the commercial (ssh.com) and the open-source (OpenSSH) clients provide helper applications called "SSH agents" that will hold the private-key passphrase in volatile memory and deliver it as needed to the SSH client program; these helper applications only need to be reinitialized when the local workstation is rebooted.

The commercial versions of the helper programs are named ssh-agent2 and ssh-add2; the open-source versions are ssh-agent and ssh-add. The details of these agents are beyond the scope of this document, but information is available through the products' documentation, help systems or man pages, Web sites, and elsewhere on the Web.

Passwords: As mentioned earlier, the MDOR SSH server does not allow users to authenticate with passwords; public-key authentication is the only method that will work. DOR recommends that you use the client GUI, Profiles/Edit Profiles/General/Defaults/Authentication (see *Figure 2)*, to make sure that "Public Key" is the only item listed in the "Authentication methods" window.

Support Information and Notes for Various SSH Client Software

We have found that most SSH clients can be made to work with DOR's SSH servers, some easily and some requiring more effort, and that a few products simply cannot be made to work with any reasonable amount of effort. In this section we will recount some of our experiences with various SSH client software products.

J2SSH

J2SSH is reported to work with DOR's SSH servers, but no further information is available.

OpenSSH

OpenSSH's sftp command is known to work with DOR's SSH servers, however the scp command will not. The syntax for OpenSSH's sftp command is different than Tectia's client, so check the documentation. The following is an example that has been reported to work:

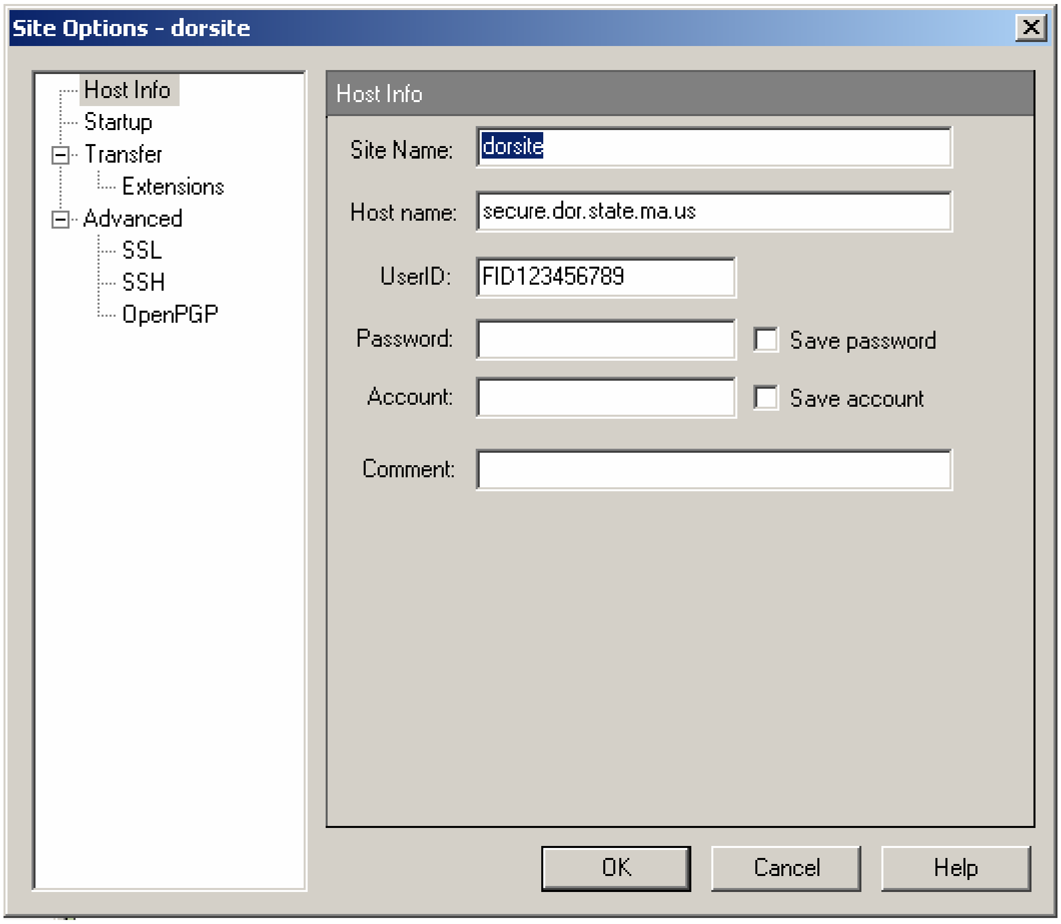
Sftp2

```
Syntax:   sftp –oPort=port -b [batchfile] [username]@[server]
Example:  sftp –oPort=444 -b work.bat FID121212121@secure.dor.state.ma.us
```

[filename]	Name of file to transfer.
[username]	FID. Example: FID121212121
[server]	DOR server = secure.dor.state.ma.us.
[port]	Port to connect to. DOR uses port 444.
[batchfile]	A file with the following FTP commands: cd download\username Get [filename] Quit

Ipswitch WS_FTP Professional 2007

WS_FTP Pro 2007 is reported to work with the DOR's SSH servers. If you use WS_FTP Pro 2007, you can create a site called, for example, "dorsite" (see Figure 12).



Site Name: dorsite

Host name: secure.dor.state.ma.us

UserID: FID123456789

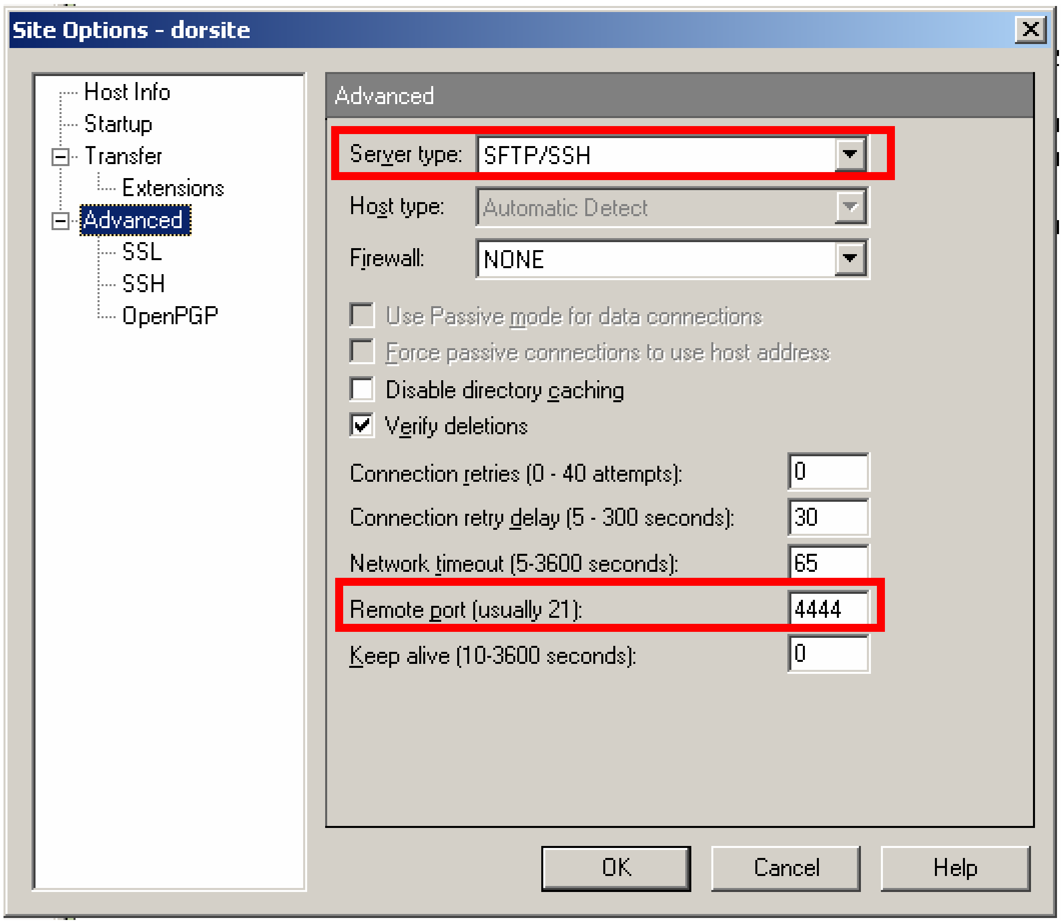
Password: □ Save password

Account: □ Save account

Comment:

Figure 12

Ensure that you've selected "SFTP/SSH" as the server type, and port "444" as the Remote port in the Advanced section (see figure 13).



Advanced

Server type: SFTP/SSH

Host type: Automatic Detect

Firewall: NONE

□ Use Passive mode for data connections

□ Force passive connections to use host address

□ Disable directory caching

☑ Verify deletions

Connection retries (0 - 40 attempts): 0

Connection retry delay (5 - 300 seconds): 30

Network timeout (5-3600 seconds): 65

Remote port (usually 21): 4444

Keep alive (10-3600 seconds): 0

Figure 13

Then create a script consisting of the following:

```
TRACE c:\temp\trace.log
LOG C:\temp\trace.log
CONNECT dorsite
PUT C:\temp\test.txt upload/test.txt
CLOSE
```

Save this script (as, say, C:\temp\test.scp), and call it like this:

```
C:\program files\ipswitch\WS_FTP Professional\ftpscrpt.com -f  c:\temp\test.scp
```

Earlier versions of WS_FTP Pro reportedly do not to work correctly with DOR's SSH servers.

Putty

Putty reportedly works with DOR's SSH servers. The following is an example that has been reported to work:

psftp

Syntax:

```
psftp –P port username@server –i [privatekey]
```

Example:

```
psftp –P 444 FID121212121@secure.dor.state.ma.us –i keyfile.key
```

[privatekey]	Path to private key
[username]	FID. Example: FID121212121
[server]	DOR server = secure.dor.state.ma.us.
[port]	Port to connect to. DOR uses port 444.

VanDyke VShell/vcp

Vcp, which is part of the VShell suite from VanDyke Software, reportedly works with DOR’s SSH servers. The following is an example that has been reported to work:

vcp

Syntax:

```
vcp -v -v -v -auth publickey –i [privatekey] -p [passphrase]
[filename] username@server#port:upload/filename
```

Example:

```
vcp -v -v -v -auth publickey –i “/home/user/.vshell/keys/mdorkey” -p
“testpassphrase” test.txt
FID121212121@secure.dor.state.ma.us#444:upload/test.txt
```

[privatekey]	Path to private key
[filename]	Name of file to transfer.
[username]	FID. Example: FID121212121
[server]	DOR server = secure.dor.state.ma.us.
[port]	Port to connect to. DOR uses port 444.

WinSCP

WinSCP is reported to work with DOR’s SSH servers, but no further information is available.

WRQ Reflection

WRQ Reflection reportedly works with DOR’s SSH servers, but no further information is available.